Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

To: The Commission

PETITION FOR RECONSIDERATION

Julie M. Kearney
Vice President, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

January 3, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Consumer Technology Association hereby petitions for reconsideration of the privacy and data security rules for broadband and telecommunications services recently adopted by the Federal Communications Commission. The Commission's partial shift to a sensitivity-based framework for carriers' use and sharing of customer information was an improvement over the approach initially proposed by the Commission, which would have represented a dramatic departure from other U.S. privacy frameworks that apply to the entire internet ecosystem. Yet while this shift brought the FCC's rules more closely in line with the Federal Trade Commission's approach, the approach ultimately adopted by the FCC still differs substantially from the time-tested FTC framework and fails to ensure a coherent and consistent approach to consumer privacy. Importantly, by classifying web browsing and application usage information that carriers collect as sensitive, and thus subject to opt-in consent for most uses and disclosures, the rules threaten to undermine the innovation and competition in the dynamic internet ecosystem that has greatly benefited consumers and the U.S. economy.

The record warranted a different approach. For example, the record included expert recommendations of the FTC staff and others urging a sensitivity-based approach entirely consistent with the FTC's approach that the Commission failed to fully consider. The Commission similarly failed to fully consider commenters' specific concerns regarding this sensitivity classification. The *Order* is further flawed because the Commission never fully contemplated the costs of its chosen approach or addressed whether its overbroad classification of sensitive information would result in anything more than illusory benefits. And finally, the *Order* is procedurally defective, given that the Commission failed to provide adequate notice of its intention to classify web browsing and application usage information as sensitive, thereby denying commenters the full opportunity for meaningful comment.

In light of these flaws, the Commission should, at minimum, revise its privacy rules to eliminate the categorization of all browsing history and application usage information as sensitive in order to ensure consistency with the FTC's longstanding and successful framework to consumer privacy. As the record made abundantly clear, the FTC's privacy approach more appropriately balances protecting consumers' privacy interests with enabling data-driven innovation.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

To: The Commission

PETITION FOR RECONSIDERATION

The Consumer Technology Association ("CTA")[1] hereby petitions for reconsideration of the Federal Communications Commission's ("Commission's" or "FCC's") *Report and Order* ("*Order*") in the above-captioned proceeding.[2] The Commission's partial shift to a sensitivity-based framework for carriers' use and sharing of customer information was an improvement over the approach proposed in the *Notice of Proposed Rulemaking* ("*NPRM*").[3] In doing so, the Commission appropriately heeded the comments of CTA and others regarding the harms of the initial proposal for broadband internet access service ("BIAS" or "broadband") and

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development, and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, WC Docket No. 16-106, FCC 16-148 (rel. Nov. 2, 2016) ("*Order*").

[3] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016) ("*NPRM*").

telecommunications providers that would have been a dramatic departure from other U.S. privacy frameworks that apply to the entire internet ecosystem.

Yet while this shift brought the FCC's rules more closely in line with the Federal Trade Commission's ("FTC's") approach than the *NPRM*, the approach ultimately adopted in the *Order* still differs substantially from the time-tested FTC framework and fails to ensure a coherent and consistent approach to consumer privacy. Importantly, by classifying web browsing and application usage information that carriers collect as sensitive, and thus subject to opt-in consent for most uses and disclosures, the rules threaten to undermine the innovation and competition in the dynamic internet ecosystem that has greatly benefited consumers and the U.S. economy.

The record warranted a different approach; the *Order* thus is flawed and merits reconsideration.[4] For example, while the record included expert recommendations of the FTC staff and others urging a sensitivity-based approach *entirely* consistent with the FTC's approach, the Commission failed to fully consider these recommendations. The Commission similarly failed to fully consider commenters' specific concerns regarding this sensitivity classification, including additional information submitted in the exceptionally short time frame between publication of the Fact Sheet[5] and the start of the "sunshine" period. More broadly, the *Order* is

[4] Although not the focus of this petition, CTA reiterates that the Commission's authority to address privacy and data security is limited to telecommunications carriers' use and protection of customer proprietary network information (as expressly defined by statute) in their provision of telecommunications services. *See* CTA Comments at 4-7; *see also* Dissenting Statement of Commissioner O'Rielly, *Order* at 212-214 (explaining the *Order*'s flawed interpretation of the FCC's privacy and data security authority, including by noting that section 222(a) does not provide independent authority to regulate privacy or data security). Nothing in the *Order* cures this legal defect, which alone supports reconsideration of the broad scope of the rules.

[5] Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information (rel. Oct. 6, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341633A1.pdf ("Fact Sheet").

flawed because the Commission never fully contemplated the costs of its chosen approach or addressed whether its overbroad classification of sensitive information would result in anything more than illusory benefits. The *Order* also is procedurally defective, given that the Commission failed to provide adequate notice of its intention to classify web browsing and application usage information as sensitive, thereby denying commenters the full opportunity for meaningful comment that the Administrative Procedure Act ("APA") requires.

In light of these flaws, the Commission should, at minimum, revise its privacy rules to eliminate the categorization of all browsing history and application usage information as sensitive in order to ensure consistency with the FTC's longstanding and successful framework to consumer privacy. As the record made abundantly clear, the FTC's privacy approach more appropriately balances protecting consumers' privacy interests with enabling data-driven innovation.

I. THE COMMISSION ERRED IN CATEGORICALLY DEFINING BROWSING HISTORY AND APP USAGE INFORMATION AS SENSITIVE

The *Order* and the record fail to justify the decision to depart from longstanding precedent and FTC recommendations with respect to what information should be considered sensitive and thus subject to opt-in consent. To the contrary, the *Order* summarily dismisses record evidence that demonstrates how the Commission could institute a sensitivity-based framework that is consistent with the FTC's framework and with the goal of providing appropriate privacy protections to consumers across the internet ecosystem.

A. THE *ORDER* IGNORES EXISTING CUSTOMER AND BUSINESS EXPECTATIONS WITH RESPECT TO THE TREATMENT OF BROWSING HISTORY AND APP USAGE INFORMATION

The *Order* fails to adequately consider existing expectations with respect to the treatment of browsing history and app usage information, most notably by failing to fully account for the

recommendations of the FTC, the primary privacy regulator and expert in the United States. The *Order* correctly observes that a sensitivity-based framework is well "calibrated to customer and business expectations."[6] The *Order* continues by noting that a sensitivity-based approach "is also consistent with the framework recommended by the FTC in its comments and its 2012 staff report, and used by the FTC in its settlements."[7] Most importantly, the *Order* appropriately finds that, compared to the *NPRM*'s approach, such a sensitivity-based framework "better reflects customer expectations regarding how their privacy is handled by their communications carrier."[8]

The *Order*, however, undermines "such customer and business expectations" by departing from the FTC's framework and existing consensus regarding what information should be considered sensitive. Specifically, the *Order* inappropriately finds that web browsing and application usage history categorically "constitute sensitive information on their own—particularly considering the comprehensiveness of collection that a BIAS provider can enjoy and the particular context of the BIAS provider's relationship with the subscriber."[9]

Importantly, the FTC *does not* consider all browser history and app usage information as sensitive personal information in its framework – the very framework that has helped to define customer and business expectations. In fact, as a coalition of advertising associations told the FCC, web browsing history and application use history have "never categorically been classified

---

[6] *Order* ¶ 173.

[7] *Id.*

[8] *Id.*; *see also* Dissenting Statement of Commissioner Ajit Pai, *Order* at 209 (The FTC's framework "reflected the uniform expectation of privacy that consumers have when they go online," which meant that "you could rest assured knowing that a single and robust regulatory approached protected your online data.") ("Pai Dissent").

[9] *Order* ¶ 181.

as 'sensitive' in *any* legislative, regulatory, or self-regulatory regime."[10] Nevertheless, the *Order* departs from such precedent without adequate justification. For example, the Commission asserts that "a user's browsing history can provide a record of her reading habits—well-established as sensitive information—as well as information about her video viewing habits, or who she communicates with via email, instant messaging, social media, and video and voice tools. Furthermore, the domain names and IP addresses may contain potentially detailed information about the type, form, and content of a communication between a user and a website."[11]

Yet, facing the exact same issue and analysis, the FTC, the premier privacy regulatory expert in the United States, declined to consider browsing history and similar information (*e.g.*, app usage information) sensitive. In its landmark 2012 privacy report, the FTC observed that one commenter in the proceeding leading up to the report had "characterized as sensitive information about consumers' online communications or reading and viewing habits," but that others "noted the inherent subjectivity of the question" and one "raised concerns about the effects on market research if the definition of sensitive data is construed too broadly."[12] Weighing these contrasting points of view, the FTC ultimately identified "general consensus regarding information about children, financial and health information, Social Security numbers, and precise geolocation data" and thus agreed that "these categories of information are

[10] The American Association of Advertising Agencies ("4A's") et al. Oct. 19, 2016 Letter at 1 (emphasis added).

[11] *Order* ¶ 183.

[12] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 57 (Mar. 2012) (citations omitted).

sensitive."[13] The FTC thus considered whether to consider browsing history and similar information as categorically sensitive, *yet ultimately declined to do so*. As Google explained, "[t]he FTC's framework recognizes that while U.S. consumers consider healthcare or financial transactions, for example, to be sensitive information that should receive special protection, they do not have the same expectations when they shop or get a weather forecast online."[14] In other words, the FTC's approach appropriately recognizes that some browsing history may be sensitive, but that consumers do not expect that all of their browsing history will be treated in the same way.

Indeed, in encouraging the FCC to shift to a sensitivity-based framework, FTC staff urged the use of opt-in only for "sensitive information that could be collected by BIAS providers."[15] In the BIAS context, FTC privacy experts specifically urged the FCC to consider the following – and only the following[16]– as sensitive:

- The content of communications;
- Social Security numbers; and
- Health, financial, children's, and precise geolocation data.[17]

---

[13] *Id.*

[14] Google Oct. 3, 2016 Ex Parte at 1; *see also, e.g.*, ITTA Oct. 21, 2016 Ex Parte at 2 (noting that "[a]gainst the backdrop of the longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information").

[15] FTC Staff Comments at 20.

[16] The *Order* claims that "[d]espite some commenters' assertions to the contrary, the FTC does not claim to define the outer bounds of sensitive information…." *Order* ¶ 178. But by classifying information as sensitive that the FTC has declined to classify as sensitive, and applying such unique classifications to BIAS, the FCC has ignored both implicit and explicit recommendations and precedent of the FTC.

[17] FTC Staff Comments at 20.

Noticeably absent from the FTC staff's recommendations is any suggestion to treat all web browsing history and app usage information as sensitive. The FTC staff could have, but did not, followed the *Order* in asserting that something unique about the relationship between broadband providers and their customers necessitated special categorization of sensitive information.[18] The FTC staff instead did the opposite, counseling against unique rules for BIAS providers – a result which the FTC staff described as "not optimal."[19]

While the Commission claims to have taken into account the recommendations of FTC staff in adopting new privacy rules for BIAS providers,[20] the *Order* ignores at least two critical recommendations by the FTC: (1) what information should be considered sensitive, and thus, by implication, what information should not be; and (2) that all online players should be subject to the same privacy and data security rules. And the *Order* does so without clearly acknowledging, let alone explaining adequately, its departure from FTC precedent and staff recommendations.

---

[18] Importantly, the *Order* states in the first instance that such information is sensitive, and then suggests it is particularly true in the broadband context. *Compare Order* ¶ 181 ("A customer's web browsing and application usage history … constitute sensitive information on their own….") *with id.* ¶ 182 ("Web browsing and application usage history, and their functional equivalents are *also* sensitive within the particular context of the relationship between the customer and the BIAS provider….") (emphasis added).

[19] *See* FTC Staff Comments at 8; *see also* Pai Dissent at 209 ("I agreed with the FTC when it said that an approach that imposes unique rules on ISPs that do not apply to all online actors that collect and use consumer data is 'not optimal.'").

[20] *See, e.g.*, *Order* ¶ 173 ("This approach is also consistent with the framework recommended by the FTC in its comments and its 2012 staff report, and used by the FTC in its settlements."); Fact Sheet at 1 ("The approach the Chairman is recommending reflects extensive public comments received in response to the comprehensive proposal adopted by the Commission in March, *including input from the Federal Trade Commission*") (emphasis added); *see also* News Release, *FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for their Personal Data* (rel. Oct. 27, 2016) ("[T]he rules establish a framework of customer consent required for ISPs to use and share their customers' personal information that is calibrated to the sensitivity of the information. This approach is consistent with other privacy frameworks, including the Federal Trade Commission's and the Administration's Consumer Privacy Bill of Rights.").

B. THE *ORDER* RELIES ON FLAWED ASSUMPTIONS REGARDING COMPANIES' ABILITIES TO LIMIT THE USE OF SENSITIVE BROWSER HISTORY AND APP USAGE INFORMATION

To justify this unacknowledged departure from the FTC's precedent and recommendations, the *Order* ignores record evidence – including the evidence parties rushed to submit in the few weeks that followed the Chairman's Fact Sheet – that overwhelmingly demonstrates how broadband providers, like any other internet player, can utilize browsing history and app usage information to deliver benefits to consumers in a manner that still protects sensitive user information.

The *Order* specifically asserts that "attempting to neatly parse customer data flowing through a network connection into sensitive and non-sensitive categories is a fundamentally fraught exercise."[21] The *Order* continues to claim that "a network provider is ill-situated to reliably evaluate the cause and meaning of a customer's network usage."[22] The *Order* is mistaken. In fact, "companies across the Internet, for decades, have used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes."[23] For example,

> ISPs can employ methods ranging from models that scan and do not log data other than whitelisted information, methods that scan and immediately delete (or not log at all) data that is identified as sensitive, or methods that log data but immediately categorize it as a high level rather than keep the underlying data. These established methods do not require companies to 'manually

[21] *Order* ¶ 187.

[22] *Id.*

[23] American Advertising Federation ("AAF") et al. Oct. 24, 2016 Letter at 1; *see also* Google Oct. 3, 2016 Ex Parte at 1 ("Google and other companies take strong measures to avoid using sensitive data for purposes like targeting ads….").

> inspect' the content of packets in order to avoid using sensitive data for targeted advertising.[24]

Moreover, while the *Order* cherry picks claims in the record that broadband providers have no way to distinguish between sensitive and non-sensitive browsing history, the *Order*'s only response to the numerous commenters that demonstrate otherwise is that "the definitions vary significantly" between industry efforts and that "[e]ven within one set of classifications, the lines between what is and is not considered sensitive information can be difficult to determine."[25] In fact, however, there is significant consensus regarding categories of information that should be considered sensitive – a fact that the *Order* simply ignores. As AT&T noted, "Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on *standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations*."[26] AT&T explained that the "process involves correlating non-content web address or app information (*e.g.*, visit to a sports website) with a pre-established 'white list' of permissible interest categories (*e.g.*, sports lover) available from the IAB" and that the "approach is used today by broadband providers and other Internet companies that use similar web browsing and app usage information for marketing purposes."[27]

---

[24] Future of Privacy Forum ("FPF") Reply Comments at 8; *see also, e.g.*, FPF Oct. 17, 2016 Ex Parte at 2; FPF Oct. 24, 2016 Ex Parte at 2.

[25] *Order* ¶ 188.

[26] AT&T Oct. 17, 2016 Ex Parte at 3 (emphasis added).

[27] *Id.*; *see also e.g.*, FTC Staff Comments at 22 n. 91 ("The prohibitions on use of sensitive information for marketing are consistent with existing approaches implemented by ad networks and mobile platforms."); Internet Commerce Coalition Oct. 18, 2016 Letter.

Further, even if there were some variance among industry standards – and there is not, because consensus exists regarding what information should be considered sensitive – the limited variance by no means would support the notion of categorically treating all browsing history or similar information as sensitive. Again, when facing the exact same issues with respect to the internet ecosystem at large, the FTC – the most experienced privacy regulator in the United States – declined to consider such information as sensitive. And more recently, FTC staff declined to urge the FCC to define such information as sensitive in the context of BIAS. Accordingly, the record simply does not support the *Order*'s claims that browsing history and app usage information inherently are sensitive, and that there are no ways to distinguish among sensitive and non-sensitive aspects of such information.

II. THE FCC ERRED BY FAILING TO PROVIDE ADEQUATE NOTICE OF ITS INTENTION TO CLASSIFY BROWSING HISTORY AND APP USAGE INFORMATION AS SENSITIVE

The proceeding that led to the *Order* was also fundamentally flawed. As parties noted to the FCC in the lead-up to the *Order*, the proposal to treat browsing history and app usage information differently from other customer information was not teed up in the *NPRM*.[28] Given that such classification departs substantially from the FTC's proven approach and the FTC staff's recommendations, the FCC erred by not seeking specific comment on the approach.

The *NPRM* never teed up treating browsing history and app usage information as sensitive. The *NPRM* instead had proposed a broad opt-in approach to virtually all customer information.[29] While parties emphasized that a sensitivity-based approach consistent with the FTC's approach – *i.e.*, an approach that subjects traditionally sensitive data, like Social Security

[28] *See, e.g.*, DMA et al. Oct. 21, 2016 Ex Parte at 1.

[29] *NPRM* ¶ 127.

numbers and geolocation information, to opt-in requirements and allows more permissive use of non-sensitive consumer data, including web browsing and app usage information – was the proper path forward,[30] parties had limited opportunity to comment specifically on the problems associated with defining web browsing and app usage information as sensitive. Parties that follow the Commission's work closely only learned that the FCC was seriously considering doing so through the Chairman's Fact Sheet, which was made public at the same time Chairman Wheeler circulated a draft order to his colleagues – by which time the Chairman had already decided on his favored approach.[31] The Fact Sheet was never published in the *Federal Register* and was issued only weeks before the vote on the order. Through ex parte presentations and letters, parties made last-minute efforts to explain the folly of defining web browsing and app usage information as sensitive, as well as the existence of a workable means of distinguishing sensitive from non-sensitive browsing and app usage history.[32]

These efforts provided valuable information to the Commission. However, the manner in which the Commission revealed its change in direction on web browsing history and app usage information and the minimal time that parties had to respond specifically to such a nuanced issue adds up to a Commission failure to provide a reasonable opportunity to comment on the

[30] *See Order* ¶ 174 n. 477 (citing FTC Staff Comments at 21-22; FPF Comments at 26; FPF Reply Comments at 8; Richard Bennett Comments at 5; ICLE Comments at 18; CompTIA Comments at 7; Internet Commerce Coalition Comments at 3; American Cable Association Comments at 51-52; State Privacy & Security Coalition Comments at 5; CenturyLink Comments at 16, 28; Comcast Comments at 13; NCTA Comments at 3; WISPA Comments at 23; INCOMPAS Comments at 12; T-Mobile Comments at 8, 29; AT&T Comments at 1, 96-97; Association of National Advertisers ("ANA") Comments at 18; FTC Commissioner Maureen Ohlhausen Comments at 1-2); *see also, e.g.*, CTA Reply Comments at 5-7.

[31] *See* Fact Sheet.

[32] *See* Section I *supra*.

proposal.[33] The *Order*'s decision to treat web browsing history and app usage information as sensitive thus is procedurally flawed, in addition to being substantively flawed.[34]

III. THE FCC FAILED TO WEIGH RECORD EVIDENCE OF THE COSTS OF CLASSIFYING WEB BROWSING HISTORY AND APP USAGE INFORMATION AS SENSITIVE

Without record support, and with only a limited opportunity for parties to weigh in on the Commission's specific approach, the *Order* simply assumes without analysis that consumers would be made better off by prohibiting broadband providers from using web browsing history and app usage information for marketing without opt-in consent. According to the *Order*, "[b]y treating all web browsing data as sensitive, we give broadband customers the right to opt in to the use and sharing of that information, while relieving providers of the obligation to evaluate the sensitivity and be the arbiter of any given piece of information."[35] The *Order*, however, never conducts a cost-benefit analysis of its overly broad classification of sensitive information, and any such analysis would fail to support the rules.

---

[33] Nevertheless, as discussed above, CTA believes that the record that preceded the Fact Sheet failed to justify such approach, and that the 11th hour record specifically on the sensitivity classification clearly demonstrates the problems associated with the *Order*'s chosen approach to browsing history and app usage information – problems the *Order* fails to fully consider.

[34] A final rule need not be identical to the original proposed rule, but when a rule "deviates too sharply from the proposal, affected parties will be deprived of notice an opportunity to respond to the proposal." *AFL-CIO v. Donovan*, 757 F.2d 330, 338 (D.C. Cir. 1985). The test is whether the final rule is a "logical outgrowth of the proposed rule" – it is not a logical outgrowth if "a new round of notice and comment would provide the first opportunity for interested parties to offer comments that could persuade the agency to modify its rule." *American Water Works Assoc. v. EPA*, 40 F.3d 1266, 1274 (D.C. Cir. 1994); *see also National Mining Ass'n v. MSHA*, 116 F.3d 520, 531 (D.C. Cir. 1997). In this context, parties were deprived of an appropriate opportunity to respond specifically to the issues associated with defining web browsing history and app usage information as sensitive. Parties' focus on that specific issue very likely would have persuaded the agency to consider otherwise.

[35] *Order* ¶ 188.

As just one record example, in an economic analysis of the FCC's initial proposal, former FTC Commissioner Joshua Wright stated:

> [T]he NPRM's one-size-fits-all regime fails to calibrate either to the sensitivity of the data at issue or to the propensity of the use at issue to cause consumer harm. It treats Social Security numbers just the same as email addresses and the selling of a consumer's information to a third-party just the same as an ISP's own use of that information…. It affords dramatically more weight to illusory privacy benefits than it does to the real and clear benefits a primarily opt-out regime offers. And it upends the current, predominate [sic] opt-out model without any consideration as to the economic costs and benefits different models offer to consumers, to firms, and to innovation.[36]

Commissioner Wright concluded that any such regime "would inflict significant direct consumer welfare losses, observable in higher prices for broadband and other services offered by ISPs, result in indirect consumer losses including a greater rate of irrelevant advertising and more expensive content and services throughout the ecosystem, and chill innovation and experimentation in the ecosystem."[37] As with a default opt-in regime, the Commission's overbroad classification of sensitive information upends the current opt-out model without considering the economic costs and benefits different models offer to consumers.

In addition, although absent in the *Order*, the record includes clear statements of the benefits of the responsible use of browsing and other online information. For example, Google noted that "consumers benefit from responsible online advertising, individualized content, and product improvements based on browsing information."[38] Likewise, representatives of the online advertising industry explained to the FCC that "[d]ata-driven online commerce and

---

[36] Joshua D. Wright, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy*, at 28-29 (May 27, 2016), attached to USTelecom May 26, 2016 Ex Parte.

[37] *Id.* at 29.

[38] Google Oct. 3, 2016 Ex Parte at 1.

advertising drive the growth of the Internet economy and deliver innovative tools and services embraced by consumers and businesses" and that this approach "subsidizes content and programming that consumers value, promotes innovation, and grows the economy."[39] In addition to these benefits, the record also demonstrated that costs of a novel, FCC-originated regulatory approach to browsing and app usage information. AT&T, for example, noted that treating browsing and app usage information as sensitive "would have far-reaching implications for the dynamic Internet economy."[40] Advertising representatives likewise observed that "expand[ing] the definition of sensitive data is likely to chill innovation and frustrate consumers as this will likely result in consumers facing a bombardment of disruptive opt-in notices"[41] and could "limit consumer choice, and ultimately harm consumers by interrupting the well-functioning Internet economy that provides consumers with free and low cost products and services."[42]

Rather than respond to these concerns, the *Order* offers only conclusory statements, without any economic rigor or analysis, regarding theoretical privacy concerns, and never

[39] 4A's et al. Oct. 24, 2016 Ex Parte at 2.

[40] AT&T Oct. 17, 2016 Ex Parte at 3; *see also* Google Oct. 3, 2016 Ex Parte at 2 ("FCC should not attempt to draw a categorical distinction between web browsing information and other information—particularly where such a novel and untested approach would unnecessarily increase regulatory burdens on the Internet.").

[41] AAF et al. Oct. 10, 2016 Letter at 4.

[42] ANA et al. Oct. 17, 2016 Ex Parte at 1; *see also* 4A's et al. Oct. 19, 2016 Letter at 1 (Defining web browsing and app usage information as sensitive "would undercut the competitive and innovative Internet marketplace, creating a negative impact on consumers and the diverse content and service offerings fostered by the responsible use of web browsing and application use history information for advertising and marketing purposes.").

identifies any potential consumer harm associated with a more permissive approach. [43] Such claims include those otherwise disproven in the record, including the notion that a broadband provider must use invasive techniques to determine whether browsing history is sensitive (as explained above in part I.B). Ultimately, the FCC's failure to conduct a cost-benefit analysis for its unproven approach – particularly in light of the evidence of the clear costs in the record and illusory nature of purported benefits – falls short of rational rulemaking. This failure of the Commission's also supports reconsideration of the *Order*.

IV. CONCLUSION

Compared to the *NPRM*'s ill-conceived initial proposal, the *Order* takes positive steps to ensure a dynamic data-driven internet ecosystem, but it does not go far enough. The Commission's decision to require BIAS providers to categorically treat web browsing and app usage information as sensitive still represents a substantial – and baseless – departure from the FTC's sound framework for the internet ecosystem. The *Order* also fails to demonstrate that its overbroad classification of sensitive information will bring benefits that outweigh the costs, which the record sets forth in detail. As a procedural matter, the Commission compounded this substantive error by failing to provide ample opportunity for interested parties to further demonstrate the folly of this approach. For these reasons, the FCC therefore should reconsider the *Order* to ensure that its rules are consistent with the FTC's longstanding and successful framework.

[43] *See, e.g.*, *Order* ¶ 184 ("The wealth of information revealed by a customer's browsing history indicates that it, even apart from communications content, deserves the fullest privacy protection.").

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION

By: */s/ Julie M. Kearney*

Julie M. Kearney
Vice President, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

January 3, 2017